

3.1 Task 1.1: Sniffing Packets

Task 1.1A

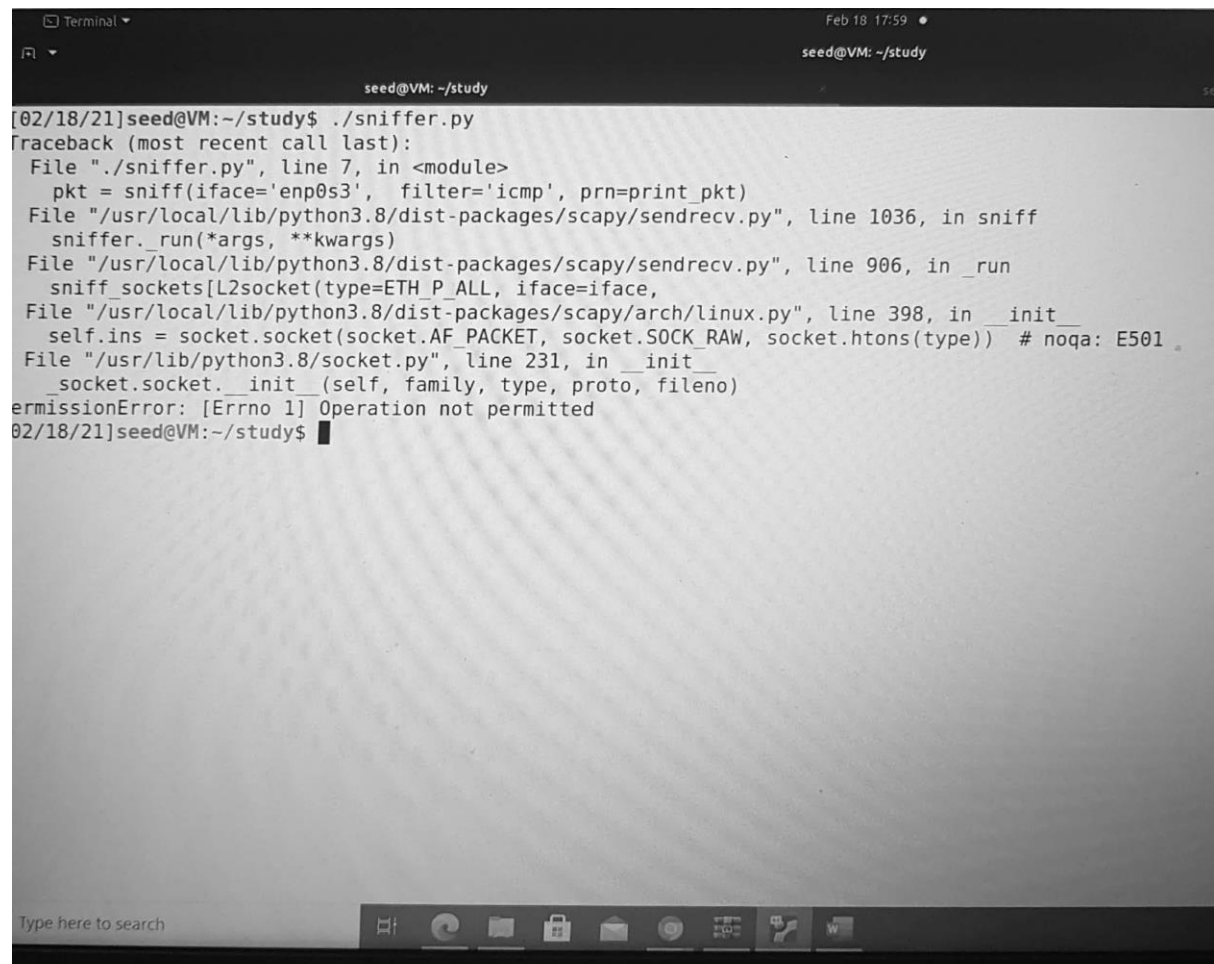
אני מריץ את התוכנית אם הROOT פריבילגיה ובתמונה רואים שהתוכנית התחילה לפעול ומחכה לקבלת או שליחת פקטות כדי להדפיס אותם

```
[02/18/21]seed@VM:~/study$ sudo ./sniffer.py
```



כאשר אני מריץ בלי רוט מקבל שגיאה

```
Feb 18 17:59 • seed@VM: ~/study
seed@VM: ~/study
[02/18/21]seed@VM:~/study$ ./sniffer.py
Traceback (most recent call last):
  File "./sniffer.py", line 7, in <module>
    pkt = sniff(iface='enp0s3', filter='icmp', prn=print_pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1036, in sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 906, in _run
    sniff_sockets[L2socket(type=ETH_P_ALL, iface=iface,
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", line 398, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type)) # noqa: E501
  File "/usr/lib/python3.8/socket.py", line 231, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[02/18/21]seed@VM:~/study$
```



Task 1.1B.

- Capture only the ICMP packet

```
seed@VM: ~/study
[02/18/21]seed@VM:~/study$ sudo ./sniffer.py
###[ Ethernet ]###
  dst      = 52:54:00:12:35:00
  src      = 08:00:27:8c:1d:fd
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 19903
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0xd0d6
  src      = 10.0.2.4
  dst      = 8.8.8.8
  \options \
###[ ICMP ]###
  type     = echo-request
  code     = 0
  chksum   = 0x8866
  id       = 0xb
  seq      = 0x1
###[ Raw ]###
  load     = '\x9f\xef.\x00\x00\x00\x00\xd5j\r\x00\x00\x00\x00\x00\x10\
!\"#$%&\'()*+,-./01234567'
###[ Ethernet ]###
  dst      = 08:00:27:8c:1d:fd
  src      = 52:54:00:12:35:00
  type     = IPv4
```

- Capture any TCP packet that comes from a particular IP and with a destination port number 23

```
SEED-Ubuntu20.04 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Feb 18 18:59
seed@VM: ~/study

[02/18/21]seed@VM:~/study$ sudo ./sniffer.py
###[ Ethernet ]###
  dst      = 52:54:00:12:35:00
  src      = 08:00:27:8c:1d:fd
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x10
  len      = 60
  id       = 23801
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = tcp
  chksum   = 0xc19f
  src      = 10.0.2.4
  dst      = 8.8.8.8
  \options \
###[ TCP ]###
  sport    = 58732
  dport    = telnet
  seq      = 1586705121
  ack      = 0
  dataoffs = 10
  reserved = 0
  flags    = S
  window   = 64240
  chksum   = 0x1c42
  urgptr   = 0
  options  = [('MSS', 1460), ('SAckOK', b''), ('Timestamp', (3925099414, 0)), ('NOP',
###[ Ethernet ]###
```

- Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16

```

[02/18/21]seed@VM:~/study$ vi sniffer.py
[02/18/21]seed@VM:~/study$ chmod a+x sniffer.py
[02/18/21]seed@VM:~/study$ sudo ./sniffer.py
#### Ethernet ####
dst      = 52:54:00:12:35:00
src      = 08:00:27:8c:1d:fd
type     = IPv4
#### IP ####
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 7625
flags    = DF
frag     = 0
ttl      = 64
proto    = icmp
chksum   = 0x8ff2
src      = 10.0.2.4
dst      = 128.230.0.4
\options \
#### ICMP ####
type     = echo-request
code     = 0
chksum   = 0xc245
id       = 0xc
seq      = 0x1
#### Raw ####
load     = '\x88\x01/\` \x00\x00\x00\x00\xbc\x03\x00\x00\x00\x00\x00\x16
1f !"#%&\ '()*+,-./01234567'
#### Ethernet ####
dst      = 52:54:00:12:35:00
src      = 08:00:27:8c:1d:fd
type     = IPv4

```

3.2 Task 1.2: Spoofing ICMP Packets

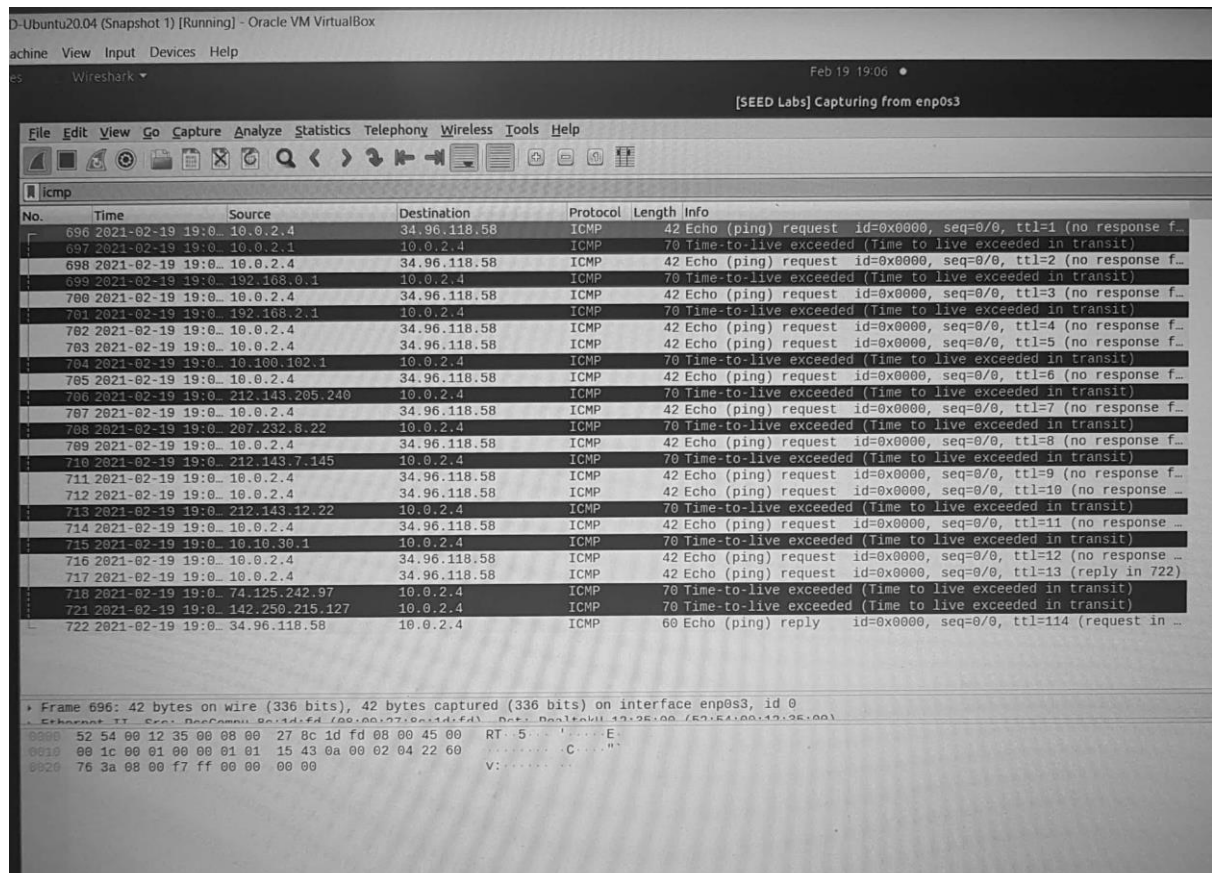
קו של המחשב שלי "10.0.2.4" החלפתי SRC ל "10.0.2.1"

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-02-19 18:00:00.000000	PcsCompu_8c:1d:fd	Broadcast	ARP	42	Who has 10.0.2.3? Tell 10.0.2.4
2	2021-02-19 18:00:00.000000	PcsCompu_df:50:10	PcsCompu_8c:1d:fd	ARP	60	10.0.2.3 is at 08:00:27:df:50:10
3	2021-02-19 18:00:00.000000	10.0.2.1	10.0.2.3	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 6)
4	2021-02-19 18:00:00.000000	PcsCompu_df:50:10	Broadcast	ARP	60	Who has 10.0.2.1? Tell 10.0.2.3
5	2021-02-19 18:00:00.000000	RealtekU_12:35:00	PcsCompu_df:50:10	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
6	2021-02-19 18:00:00.000000	10.0.2.3	10.0.2.1	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=255 (request in ...)

3.3 Task 1.3: Traceroute

בתמונה מלמטה כל IP של נתבים שאני עובר כדי להגיע עד IP של אוניברסיטת אריאל ש IP שלה

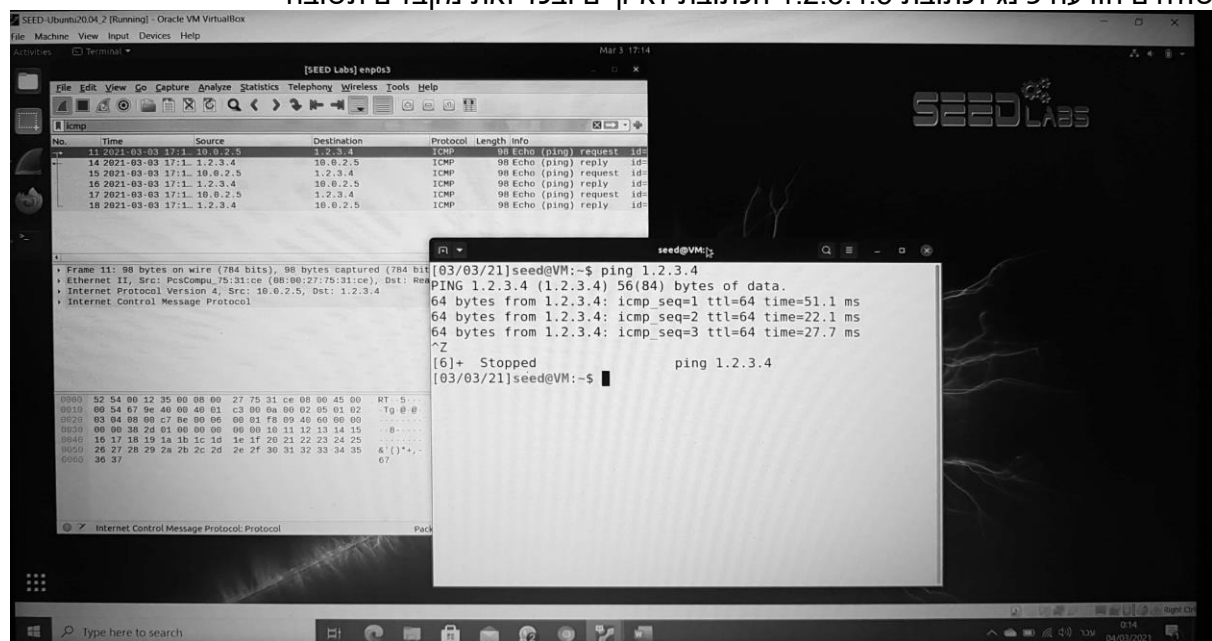
"34.96.118.58"



Scanned with CamScanner

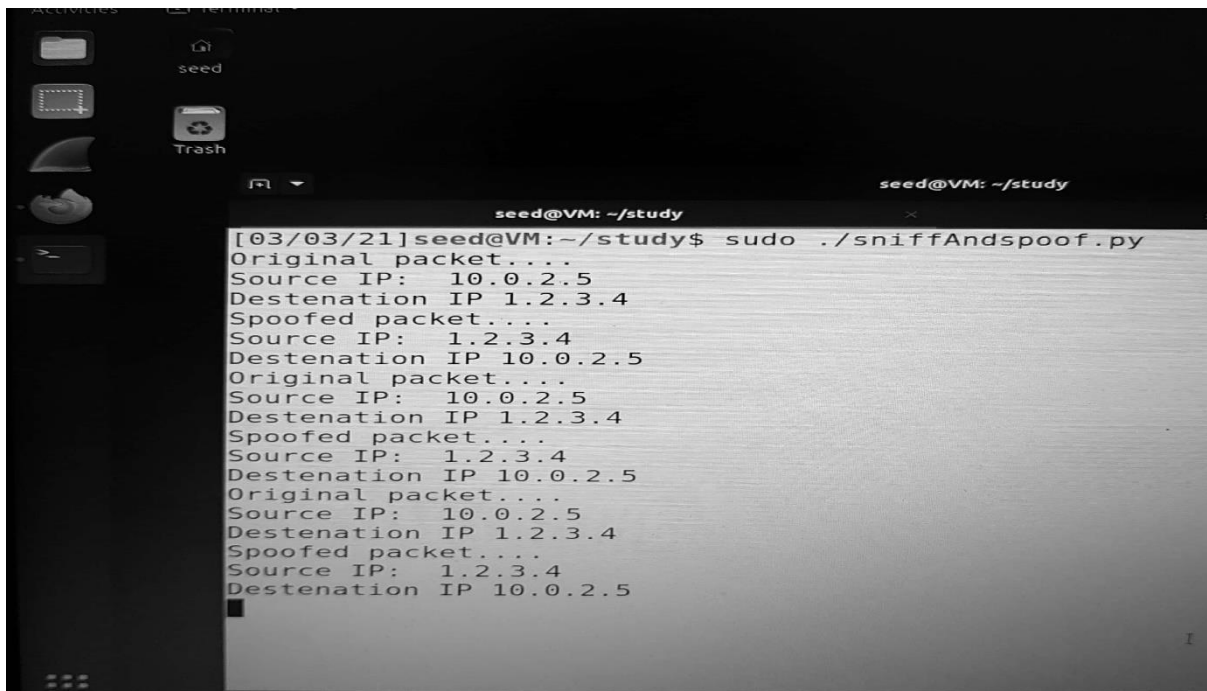
3.4 Task 1.4: Sniffing and then Spoofing

שולחים הודעה פינג לכתובת 1.2.3.4.5 הכתובת לא קיים ובכל זאת מקבלים תשובה



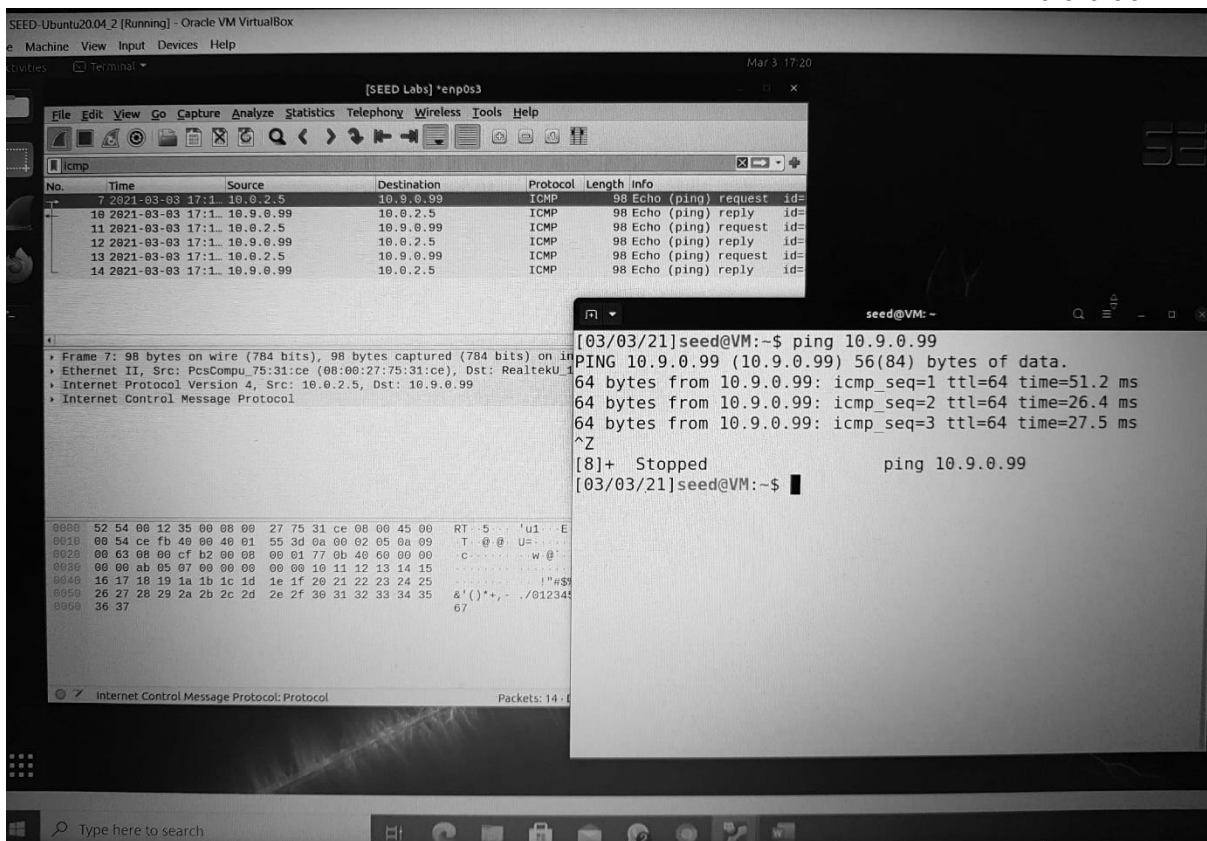
Scanned with CamScanner

סניפר נכתב כך שהוא מזהה שמהכתובת 10.0.2.5 שולחים הודעה פינג ושולח לו תשובה אפילו אם לא קיים הכתובת הזאת



```
seed@VM: ~/study
[03/03/21]seed@VM:~/study$ sudo ./sniffAndspoof.py
Original packet....
Source IP: 10.0.2.5
Destination IP 1.2.3.4
Spoofed packet....
Source IP: 1.2.3.4
Destination IP 10.0.2.5
Original packet....
Source IP: 10.0.2.5
Destination IP 1.2.3.4
Spoofed packet....
Source IP: 1.2.3.4
Destination IP 10.0.2.5
Original packet....
Source IP: 10.0.2.5
Destination IP 1.2.3.4
Spoofed packet....
Source IP: 1.2.3.4
Destination IP 10.0.2.5
```

פינג ל10.9.0.99



SEED- Ubuntu20.04.2 [Running] - Oracle VM VirtualBox

Machine View Input Devices Help

Activities [Terminal]

[SEED Labs] *enpos3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

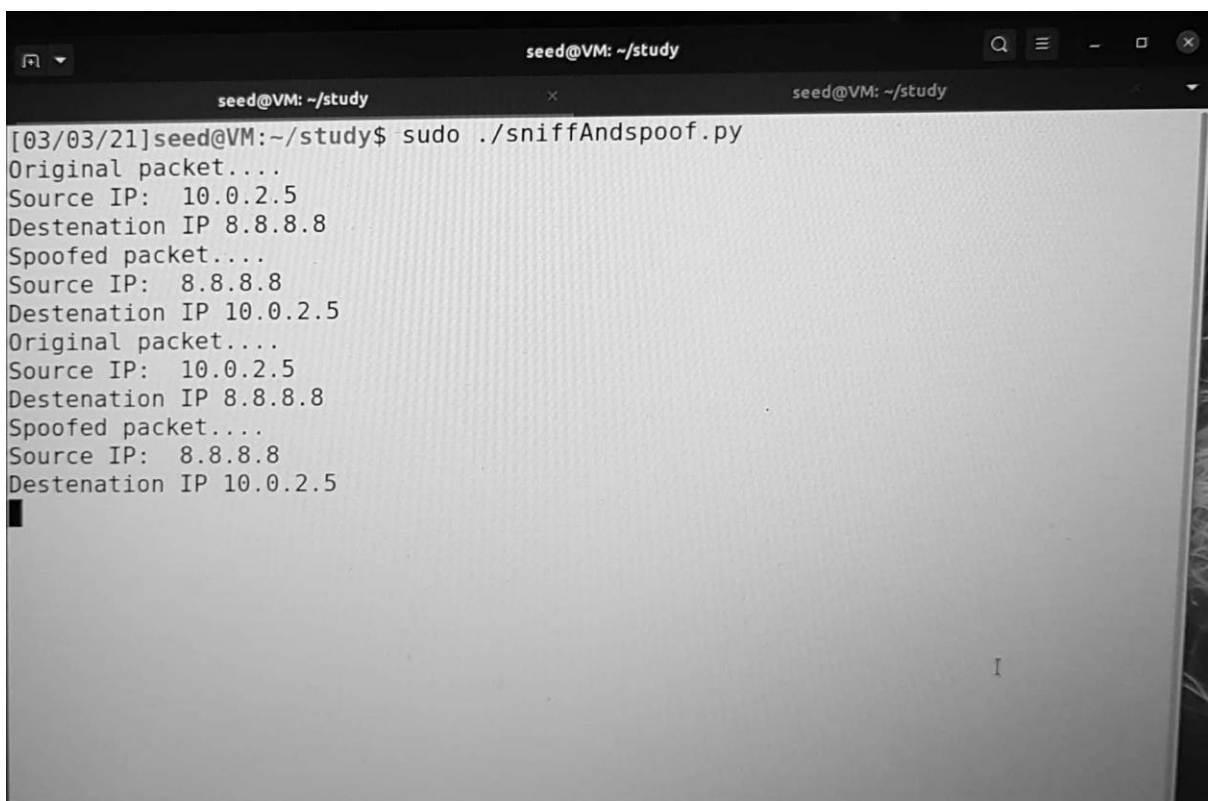
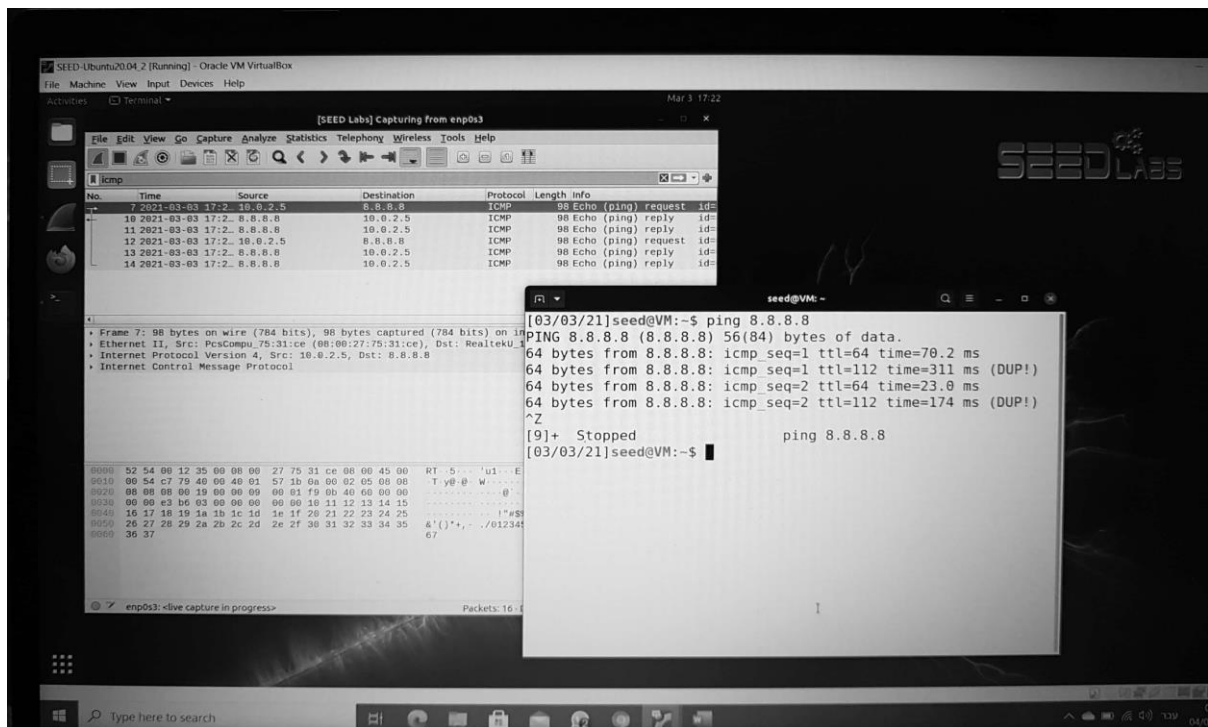
No.	Time	Source	Destination	Protocol	Length	Info
7	2021-03-03 17:11:10.03215	10.9.0.99	10.0.2.5	ICMP	98	Echo (ping) request id=
10	2021-03-03 17:11:10.03215	10.9.0.99	10.0.2.5	ICMP	98	Echo (ping) reply id=
11	2021-03-03 17:11:10.03215	10.9.0.99	10.0.2.5	ICMP	98	Echo (ping) request id=
12	2021-03-03 17:11:10.03215	10.9.0.99	10.0.2.5	ICMP	98	Echo (ping) reply id=
13	2021-03-03 17:11:10.03215	10.9.0.99	10.0.2.5	ICMP	98	Echo (ping) request id=
14	2021-03-03 17:11:10.03215	10.9.0.99	10.0.2.5	ICMP	98	Echo (ping) reply id=

Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface
Ethernet II, Src: PcsCompu.75:31:ce (08:00:27:75:31:ce), Dst: RealtekU
Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.9.0.99
Internet Control Message Protocol

```
seed@VM: ~$ ping 10.9.0.99
PING 10.9.0.99 (10.9.0.99) 56(84) bytes of data:
64 bytes from 10.9.0.99: icmp_seq=1 ttl=64 time=51.2 ms
64 bytes from 10.9.0.99: icmp_seq=2 ttl=64 time=26.4 ms
64 bytes from 10.9.0.99: icmp_seq=3 ttl=64 time=27.5 ms
^Z
[8]+  Stopped                  ping 10.9.0.99
[03/03/21]seed@VM:~$
```


שולחים הודעה פינג לכתובת 8.8.8.8 למרות שהכתובת קיים הסניפר מזהה שמהכתובת 10.0.2.5 נשלחה

הודעה ו- spoof שולח תשובה



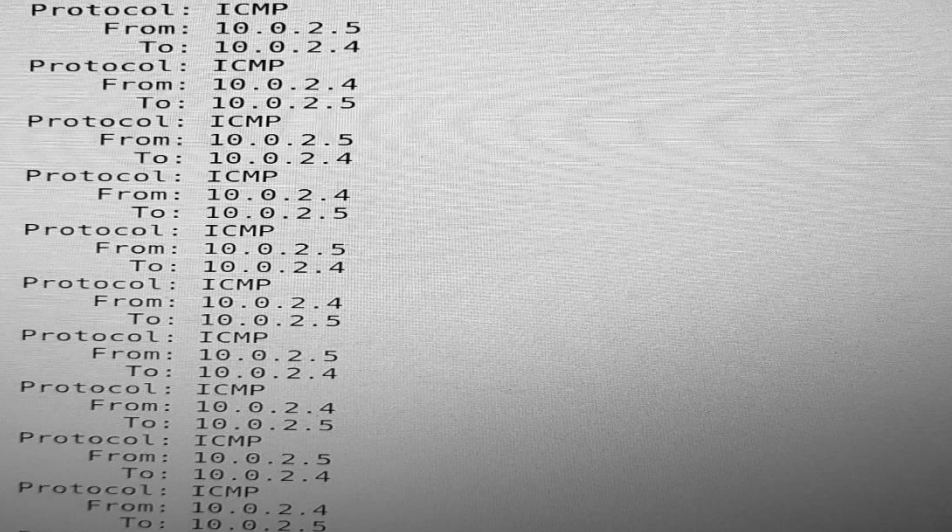
Task 2.1A:

```
[03/04/21]seed@VM:~/study$ sudo ./sniff
From: 10.0.2.4
To: 35.224.170.84
Protocol: TCP
From: 10.0.2.4
To: 10.0.2.3
Protocol: UDP
From: 10.0.2.3
To: 10.0.2.4
Protocol: UDP
From: 35.224.170.84
To: 10.0.2.4
Protocol: TCP
From: 10.0.2.4
To: 35.224.170.84
Protocol: TCP
From: 10.0.2.4
To: 35.224.170.84
Protocol: TCP
From: 35.224.170.84
To: 10.0.2.4
Protocol: TCP
From: 35.224.170.84
To: 10.0.2.4
Protocol: TCP
From: 35.224.170.84
To: 10.0.2.4
Protocol: TCP
From: 10.0.2.4
To: 35.224.170.84
Protocol: TCP
From: 10.0.2.4
To: 35.224.170.84
Protocol: TCP
```

Scanned with CamScanner

1. התוכנית sniff.c מזהה איזה ממשק נרצה לרחרח באמצעות pcap_lookupdev אם המשתמש לא מכניס את הממשק ניתן לזהות על ידי מספר הרשת לאחר מכן מאותחל pcap ומתחילים לרחרח.
2. אנחנו צריכים הרשאת root כדי שנוכל הריץ את sniff כיון שהתוכנית מרחרחת עבור ממשק שדורש הרשאות אלו, אם לא יהיה לנו הרשאת root זה יכשל ב pcap_open_live שננסה לפתוח את הממשק ונקבל את השגיאה הבאה לא ניתן לפתוח את המכשיר כי אין לך הרשאה.
3. מתי ש- promiscuous mode נמצא במצב 0 ואין תעבורת רשת ה-sniff לא ימצא שום דבר, ומתי שניהיה במצב 1 גם אם אין תעבורת רשת עדיין ה-sniff ירחרח.

- Capture the ICMP packets between two specific hosts.



```
[3/04/21]seed@VM:~/study$ sudo ./sniff
  From: 10.0.2.4
  To: 10.0.2.5
  Protocol: ICMP
  From: 10.0.2.5
  To: 10.0.2.4
  Protocol: ICMP
  From: 10.0.2.4
  To: 10.0.2.5
  Protocol: ICMP
  From: 10.0.2.5
  To: 10.0.2.4
  Protocol: ICMP
  From: 10.0.2.4
  To: 10.0.2.5
  Protocol: ICMP
  From: 10.0.2.5
  To: 10.0.2.4
  Protocol: ICMP
  From: 10.0.2.4
  To: 10.0.2.5
  Protocol: ICMP
  From: 10.0.2.5
  To: 10.0.2.4
  Protocol: ICMP
  From: 10.0.2.4
  To: 10.0.2.5
  Protocol: ICMP
  From: 10.0.2.5
  To: 10.0.2.4
  Protocol: ICMP
```


- Capture the TCP packets with a destination port number in the range from 10 to 100.

[illegible]

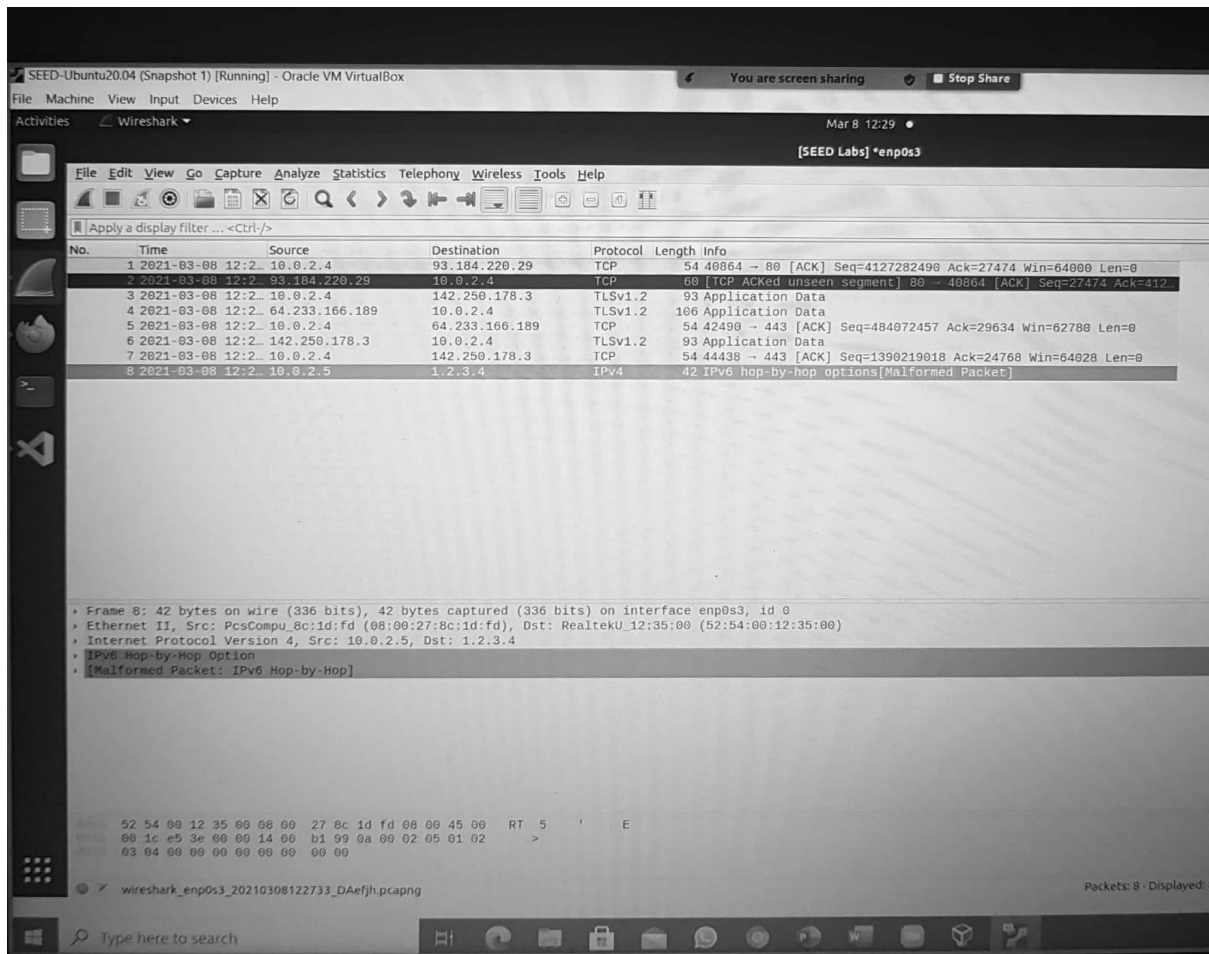
Task 2.1C: Sniffing Passwords (dees)

```
Activities Terminal
get packet
  From: 10.0.2.4
  To: 10.0.2.5
  Source port: 32994
  Destination port: 23
  Protocol: TCP
  payload (13 bytes):
00000000B0E0d
get packet
  From: 10.0.2.4
  To: 10.0.2.5
  Source port: 32994
  Destination port: 23
  Protocol: TCP
  payload (13 bytes):
00000000B0IQe
get packet
  From: 10.0.2.4
  To: 10.0.2.5
  Source port: 32994
  Destination port: 23
  Protocol: TCP
  payload (13 bytes):
00000000B0J0e
get packet
  From: 10.0.2.4
  To: 10.0.2.5
  Source port: 32994
  Destination port: 23
  Protocol: TCP
  payload (13 bytes):
00000000gB0M0s
get packet
  From: 10.0.2.4
  To: 10.0.2.5
```

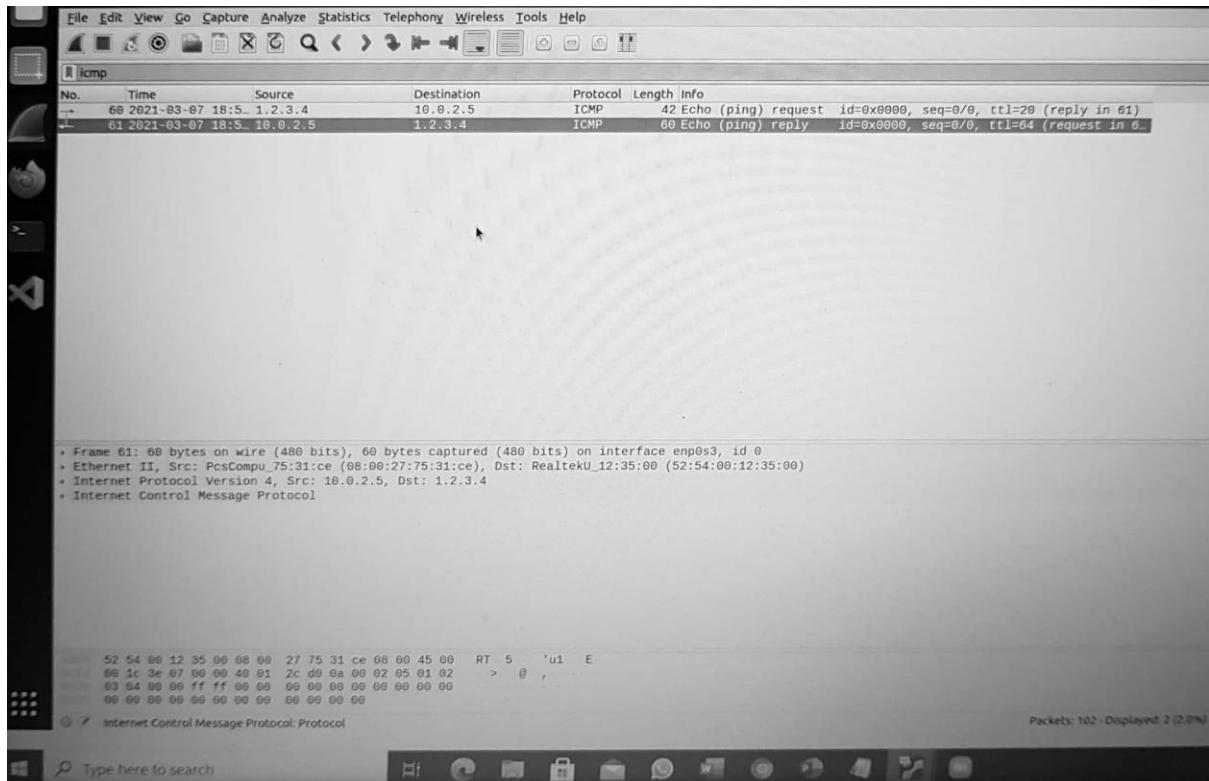
Task 2.2: Spoofing

2.2A

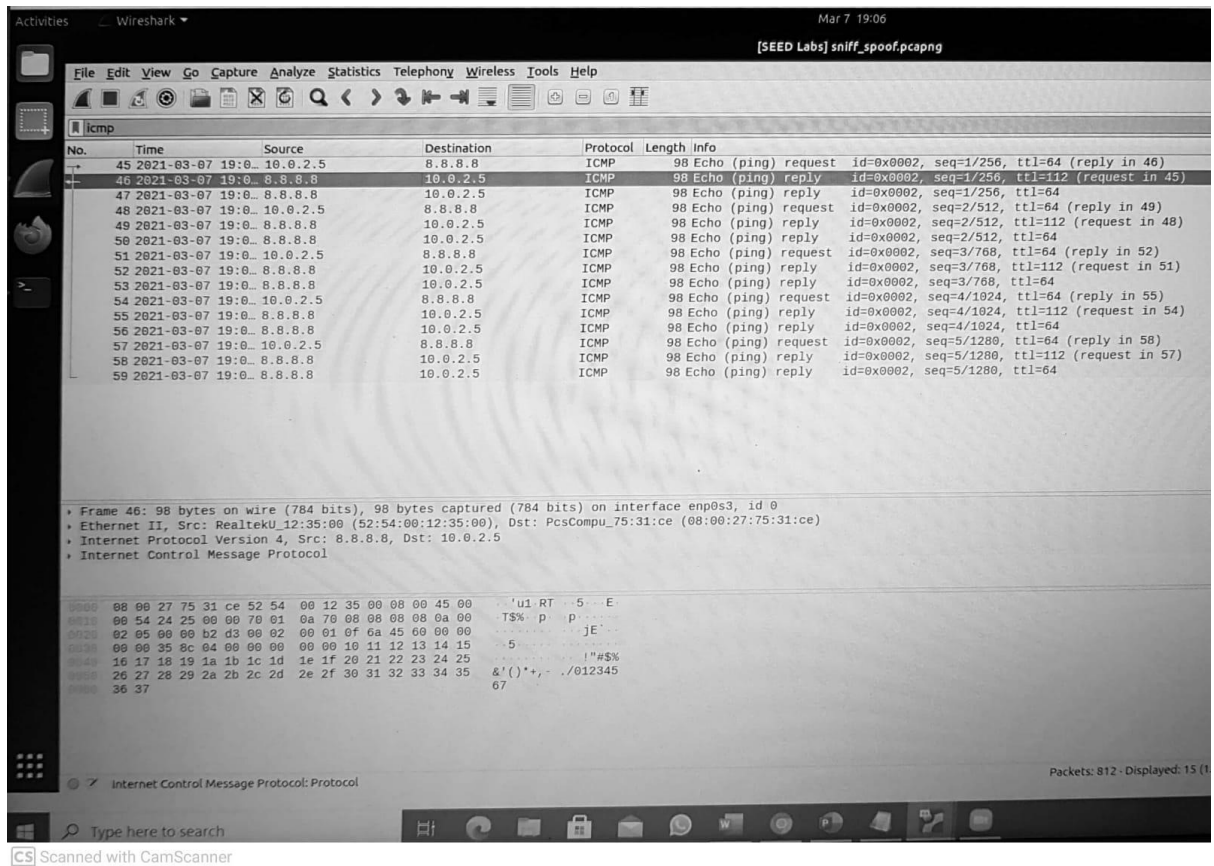
Spoof ip



Spoof an ICMP Echo Request



Task 2.3: Sniff and then Spoof



4. כן ניתן להגדיר קו ללא קשר לגודל החבילה.

5. כן כדי להתחמק משגיאות.

6. למשתמש רגיל אין אישור לפתוח socet ולכן זה נכשל שם.